SOPHOS

Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector

How root cause impacts ransomware outcomes based on insights from 2,974 organizations hit by ransomware in the past year.

A Sophos Whitepaper. April 2024

Introduction

To deploy a ransomware attack, adversaries must first gain access to a victim's corporate environment, devices, and data. Threat actors typically use two main approaches to gain entry: logging in using **compromised credentials**, i.e., legitimate access data that had previously been stolen, and **exploiting vulnerabilities** in applications and tools used by the business. Other less common modes of entry include brute force attacks, supply chain compromise, malicious emails/documents, and adware. Phishing features heavily in ransomware attacks but is primarily used to steal the credentials later used to log in to the organization.

This report highlights how ransomware outcomes differ depending on the root cause of the attack. It compares the severity, financial cost, and operational impact of attacks that start with an exploited vulnerability with those where adversaries use compromised credentials to penetrate the organization. It also identifies the industry sectors most and least commonly exploited.

The findings are based on a vendor-agnostic survey commissioned by Sophos of 2,974 IT/cybersecurity professionals in small and mid-sized organizations (100-5,000 employees) that had been hit by ransomware in the last year. The study was conducted by independent research agency Vanson Bourne in early 2024 and reflects respondents' experiences over the previous 12 months.

Executive summary

While all ransomware attacks have negative outcomes, those that start by exploiting unpatched vulnerabilities are particularly brutal for their victims. Organizations hit by attacks that began in this way report considerably more severe outcomes than those whose attacks started with compromised credentials, including a higher propensity to:

- Have backups compromised
  (75% success rate vs. 54% for compromised credentials)
- Have data encrypted
  (67% encryption rate vs. 43% for compromised credentials)
- Pay the ransom
  (71% payment rate vs. 45% for compromised credentials)
- Cover the full cost of the ransom in-house
  (31% funded the full ransom in-house vs. 2% for compromised credentials)

They also reported:

- 4X higher overall attack recovery costs
  ($3M vs. $750k for compromised credentials)
- Slower recovery time
  (45% took more than a month vs. 37% for compromised credentials)

The study focuses on correlation, and further exploration is needed into reasons behind these outcomes. It's important to bear in mind that not all ransomware attacks are equal. Some are executed by sophisticated, well-funded gangs using a range of innovative approaches. At the same time, the use of crude, cheap ransomware by lower-skilled threat actors is on the rise. It may be that adversaries that are able to exploit unpatched software vulnerabilities are more skilled than attackers who buy stolen credentials from the dark web (for example), and therefore better able to succeed in compromising backups and encrypting data.

Learning 1: One-third of ransomware attacks start with an unpatched vulnerability

32% of ransomware attacks experienced by the survey respondents in the past year started with an exploited vulnerability. Diving deeper, we see that the proportion of ransomware attacks that began in this way varies considerably by industry:

- Highest: energy, oil/gas, and utilities – 49% of attacks
- Lowest: construction and property – 21% of attacks

This variation is likely impacted, in part, by the different technology solutions used and their associated patching challenges. Sectors such as energy, oil/gas, and utilities typically use a higher proportion of older technologies more prone to security gaps than many other sectors. and patches may not be available for legacy and end-of-life solutions.

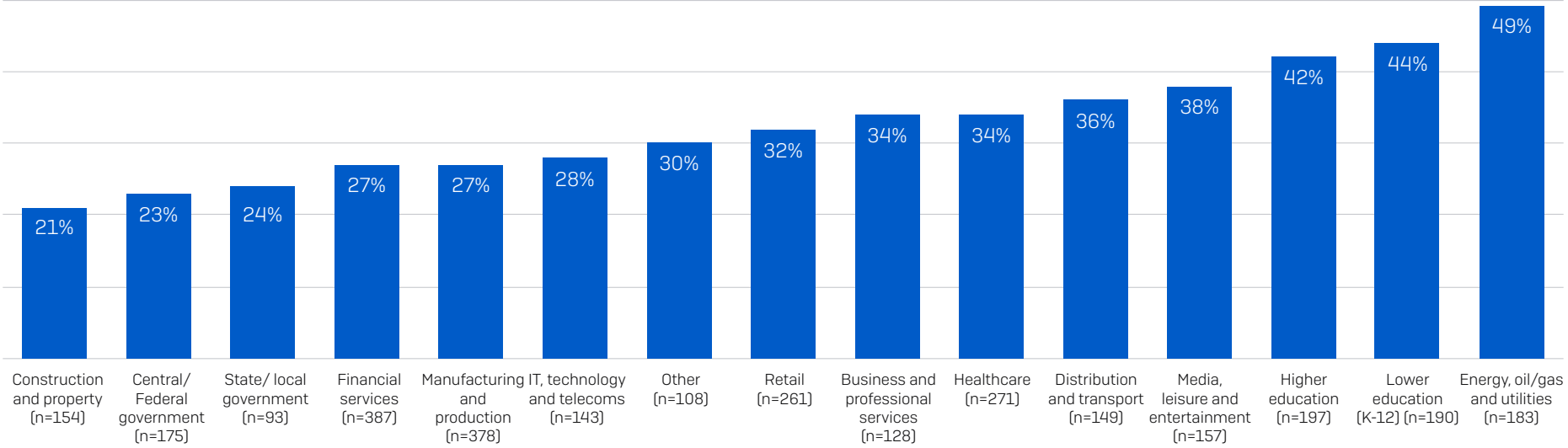
At the same time, more often than not, patches are available – they just haven't been applied. Of the attacks that Sophos incident responders were brought in to remediate in 2022 that started with exploited vulnerabilities, over half (55%) were caused by ProxyShell and Log4Shell — both of which had existing patches at the time of compromise. Sophos continues to see ProxyShell being exploited 30 months after the release of the patch. Learn more.

The analysis also revealed that the propensity to experience an exploit-led attack varies by organization size:

- 26% of ransomware attacks in small businesses (sub $50M annual revenue)
- 30% of ransomware attacks in mid-sized businesses ($50M-$1B)
- 37% of ransomware attacks in large businesses ($1B+)

As organizations grow, their IT infrastructures tend to grow with them. The larger the environment, the greater the challenge in understanding the attack surface and the more tools and technologies that need to be maintained.

Percentage of attacks that started with exploited vulnerability



Learning 2: Ransomware impacts are more severe when the attack starts with an exploited vulnerability

The final goal for a ransomware actor is to encrypt an organization's data and extract a ransom payment in return for the decryption key. On the way, they almost always attempt to compromise their victim's backups to reduce their ability to restore data without paying.

The analysis reveals that across all three points – backup compromise, data encryption, and ransom payment – the impacts are most severe when the attack starts with an exploited vulnerability.

Backup compromise

There is no difference in attackers' propensity to attempt to compromise backups based on the root cause. Adversaries tried to compromise them in 96% of attacks that started with exploited vulnerabilities and compromised credentials. However, there is a considerable difference in their success rate:

- 75% of attempts were successful when the attack started with an exploited vulnerability
- 54% of attempts were successful when the attack started with compromised credentials

This may be because adversaries who leverage unpatched vulnerabilities are more skilled at breaching backups. It may also reflect that organizations with an exposed attack surface have weaker backup protection. Whatever the cause, having your backups compromised reduces resilience against the full impact of the attack.

Data encryption

Organizations are more than 50% more likely to have their data encrypted when an attack starts with an exploited vulnerability rather than compromised credentials:

- 67% of attacks resulted in data encryption when the attack started with an exploited vulnerability
- 43% of attacks resulted in data encryption when the attack started with compromised credentials

As with backup compromise, the difference in outcome by root cause may reflect differing skill levels in adversary groups and differences in the overall strength of an organization's cyber defenses.

Ransom payment rate

Given the higher rate of backup compromise reported when the attack started with an exploited vulnerability, it's perhaps no surprise that this group reported a higher propensity to pay the ransom:

- 71% of organizations that had data encrypted paid the ransom when the attack started with an exploited vulnerability
- 45% of organizations that had data encrypted paid the ransom when the attack started with compromised credentials

Without backups to recover from, the pressure on ransomware victims to access the decryption key increases, likely driving organizations to work with the attackers to restore data.

Learning 3: Unpatched vulnerabilities have business-critical consequences

Ransomware attacks that start with an exploited vulnerability have considerably greater financial and operational impact than those that begin with compromised credentials.

Ransom payment

While the attack root cause has an almost negligible impact on the ransom payment sum, with the median amount coming in at $1.988M (exploited vulnerabilities) and $2M (compromised credentials), it does have a considerable impact on the funding of the ransom payment:

- 31% of organizations funded the full ransom in-house when the attack started with an exploited vulnerability
- 2% of organizations funded the full ransom in-house when the attack started with compromised credentials

Parent companies and cyber insurance providers are more likely to contribute to the ransom when the attack starts with compromised credentials rather than an exploited vulnerability.

Looking more broadly at the propensity of insurance carriers to honor claims we see that one quarter (25%) of denied claims by organizations that experienced an exploited vulnerability were due to not having the required cyber defenses for the claim to be honored, compared to 12% of claims where adversaries used compromised credentials.

Recovery cost

The ransom is just one element that contributes to the overall recovery cost from a ransomware attack. Leaving aside any ransom paid, the median overall recovery cost for ransomware attacks that start with an exploited vulnerability ($3M) is four times greater than for those that begin with compromised credentials ($750K).

Recovery time

Recovering from an attack that starts with an exploited vulnerability is typically much slower than when the root cause is compromised credentials.

- 45% took more than a month to recover when the attack started with an exploited vulnerability
- 37% took more than a month to recover when the attack started with compromised credentials

This finding likely reflects the different remediation activities that victims need to undertake depending on the root cause, and their respective operational overheads. Patching a system or upgrading from an end-of-life product to a supported version may well be more time-consuming than resetting credentials. It may also be a result of the greater damage caused by exploited vulnerability attacks, including a greater likelihood of backup compromise and data encryption.

Recommendations

Patching is a vital first step in reducing the risk of falling victim to a ransomware attack (or any other breach) that starts with an exploited vulnerability. If you fix the security gap, adversaries can't exploit it. Patching should ideally be part of a broader exploit-prevention risk management strategy.

Minimize your attack surface

- Maintain full visibility of all your external-facing assets to know what you're dealing with and avoid blind spots.
- Patch using risk-based prioritization. With new exploits discovered faster than most organizations can fix them, focus your efforts where they will have the most impact. This means identifying and prioritizing the patching of high-risk exposures.
- Update regularly. Using the latest version of an application or tool ensures you benefit from the vendors' most recent security fixes.

Deploy anti-exploit protections

While the number of exploitable vulnerabilities continues to grow rapidly, attackers can only leverage a limited number of techniques to exploit. Built-in anti-exploitation capabilities in endpoint security solutions stop the behaviors used in these attacks – including with zero-day vulnerabilities for which no patch has yet been released.

Detect and respond to suspicious activities

Technology alone cannot stop every attack. Adversaries are skilled at leveraging legitimate IT tools and stolen credentials, adapting their approach on the fly to avoid detection. Stopping advanced, human-led ransomware attacks and breaches requires 24/7 detection and response across your environment, delivered by a specialist provider or highly-skilled in-house team.

How Sophos can help

Sophos Managed Risk

Sophos Managed Risk is a vulnerability and attack surface management service powered by industry-leading Tenable technology and delivered by a dedicated team of Sophos threat exposure and remediation experts. It addresses four critical use cases: attack surface visibility, continuous risk monitoring, vulnerability prioritization, and fast identification of new risks.

Sophos Managed Risk is available with Sophos MDR, a fully managed cybersecurity service delivered 24/7 by Sophos threat experts. A dedicated team of Sophos Managed Risk operators – highly skilled in vulnerabilities and threat exposures - works closely with Sophos MDR analysts around the clock. Learn more.

Sophos Endpoint

Sophos Endpoint includes more than 60 anti-exploitation capabilities that block the behaviors adversaries use to exploit an unpatched vulnerability, stopping both known vulnerabilities and zero-day threats. The anti-exploit capabilities deploy automatically from day one with no configuration or need for fine tuning.

Sophos Endpoint takes a comprehensive approach to protection without relying on one security technique. Web, application, and peripheral controls reduce your threat surface and block common attack vectors. AI, behavioral analysis, anti-ransomware, and other state-of-the-art technologies stop threats fast before they escalate. Learn more.

2024-03-27 (WP-PC)

SOPHOS